

Towards $P = NP$ via k-SAT: A k-SAT Algorithm Using Linear Algebra on Finite Fields

© Matt Groff 2011

SEMI-COMPLETE FIRST DRAFT

MATT GROFF

P.O. Box 642

Camp Hill, PA, USA 17001-0642

mgroff100@hotmail.com

January 27, 2013

Abstract

The problem of P vs. NP is very serious, and solutions to the problem can help save lives. This article is an attempt at solving the problem using a computer algorithm. It is presented in a fashion that will hopefully allow for easy understanding for many people and scientists from many diverse fields.

In technical terms, a novel method for solving k-SAT is explained. This method is primarily based on linear algebra and finite fields. Evidence is given that this method may require roughly $O(n^3)$ time and space for deterministic models. More specifically the algorithm runs in time $O(P \cdot V(n + V)^2)$ with mistaking satisfiable Boolean expressions as unsatisfiable with an approximate probability $1/\Theta(V(n + V)^2)^P$, where n is the number of clauses and V is the number of variables. It's concluded that significant evidence exists that $P=NP$.

There is a forum devoted to this paper at <http://482527.ForumRomanum.com>. All are invited to correspond here and help with the analysis of the algorithm. Source code for the associated algorithm can be found at <https://sourceforge.net/p/la3sat>.

fundamental question in computer science is to find if certain types of problems, collectively known as the class NP, can be solved quickly by a computer. If so, a world of opportunities would open up, and many new problems that were supposed to be almost impossible to solve could be solved quickly. This paper attempts to provide a proof that they can be solved quickly, and also shows a way to do it. This will hopefully invite researchers from many diverse fields to contribute to the research and work of solving NP hard problems.

The level of interest in this question is so great that in 2000, the Clay Mathematics Institute listed the 7 Millennium Prize Problems, and offered \$1,000,000 for someone who could prove the relationship between P and NP[7], which would answer the question.

1.1 Turing Machines

To understand the classes P and NP, first consider the basic notion of a Turing machine, which is a scientific definition of a computer. It has one or more tapes that hold information. At any time, the Turing machine uses the tape or tapes to decide what to do next. The machine has a prescribed set of instructions to it to help it decide.

To develop the ideas behind Turing machines more, a distinction is made between what types of decisions can be made. A deterministic Turing machine (DTM) has a predetermined decision for every type of situation it encounters; thus the term deterministic. A nondeterministic Turing machine (NTM), on the other hand, can have more than one action it can do for any given situation. In other words, it's actions aren't determined ahead of time. Therefore, it's said that it's nondeterministic.

Figure 1 makes the difference more clear. NTMs

1 Introduction

There are many problems proposed to computer scientists that have been thought to be too difficult for computers to solve quickly. In fact, perhaps the most

A decision tree is shown below. As an algorithm (computer program) progresses, it must pick a choice from three possibilities. Nondeterministic turing machines(NTMs) have been thought to have an advantage in this case, because, at each step, they can pick from any choice. Deterministic turing machines(DTMs) don't really have the ability to pick, so they're thought to be at a disadvantage.

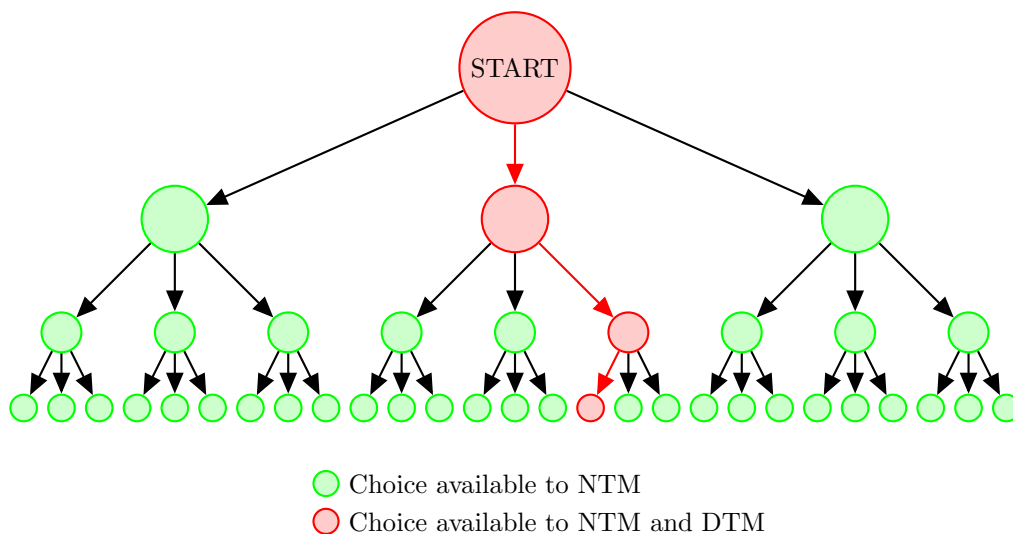


Figure 1: A Scenario Involving Choices

have been thought to be able to solve more problems than DTMs because of the availability to make more choices. Here the DTM has only one choice available at each step, while the DTM has three choices available. So this evidence points to DTMs as being more limited in potential than NTMs. In fact, there is enough difference between these two computers that different classes of computation (computational power) were proposed for each.

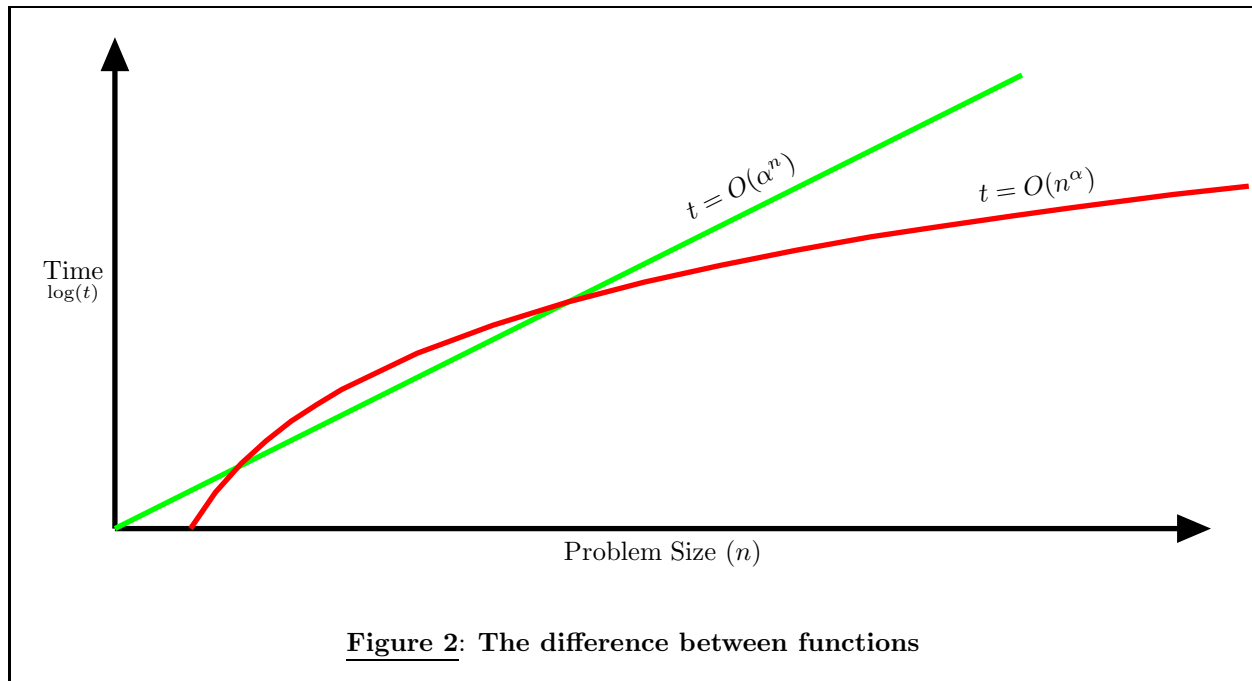
1.2 P and NP

Right around 1970, Leonid Levin, in the USSR, and Stephen Cook, of the US, independently arrived at the concept of NP-completeness[1].

The idea of NP-completeness comes from two classes of algorithms. Once again, these two classes come from the ideas of DTMs and NTMs.

The classes are defined partially by how much can be accomplished within a limited amount of time. This time limit, which will be explained briefly here, is defined by the mathematics of asymptotic analysis, which is described in [10]. Basically, the time limit is given as a function of the problem size. The function can take on many forms, and two common forms are shown above in Figure 2. Here a polynomial function ($t = O(n^\alpha)$) is contrasted with an exponential function ($t = O(\alpha^n)$). Note that the polynomial functions may take more time for smaller problems, but the larger problems, which computer scientists are mainly concerned with, have smaller times for polynomial functions.

The two classes mentioned above are defined for polynomial functions. One class, P , is defined as all problems that can be solved by a DTM in polynomial time (a polynomial function of the problem size). The



other class, NP , is defined as the class of all problems that can be solved by an NTM in polynomial time. NP -complete problems are then problems in NP that are at least as hard to solve as the hardest problems in NP .

The fundamental question that this paper attempts to answer is if NP -complete problems can be solved in polynomial time by a DTM; in other words, is $P = NP$?

For more information on P versus NP , one can refer to Sipser [6].

1.3 SAT and k -SAT

SAT essentially asks if, given a Boolean formula, can the formula be satisfied. In other words, it asks if the variables in the formula be given a truth assignment that makes the entire formula true. It's required, to thoroughly answer the question, that a certificate is given if the answer is true. This is usually in the form of a particular solution to the question, such as a satisfying assignment for all variables.

k -SAT is a particular variation of SAT, in which the formula is organized into clauses. All variables inside a clause are connected via disjunction. All clauses are connected via conjunction. The k in k -SAT then refers to the number of variables in each clause. More information on SAT and k -SAT can be found in [12].

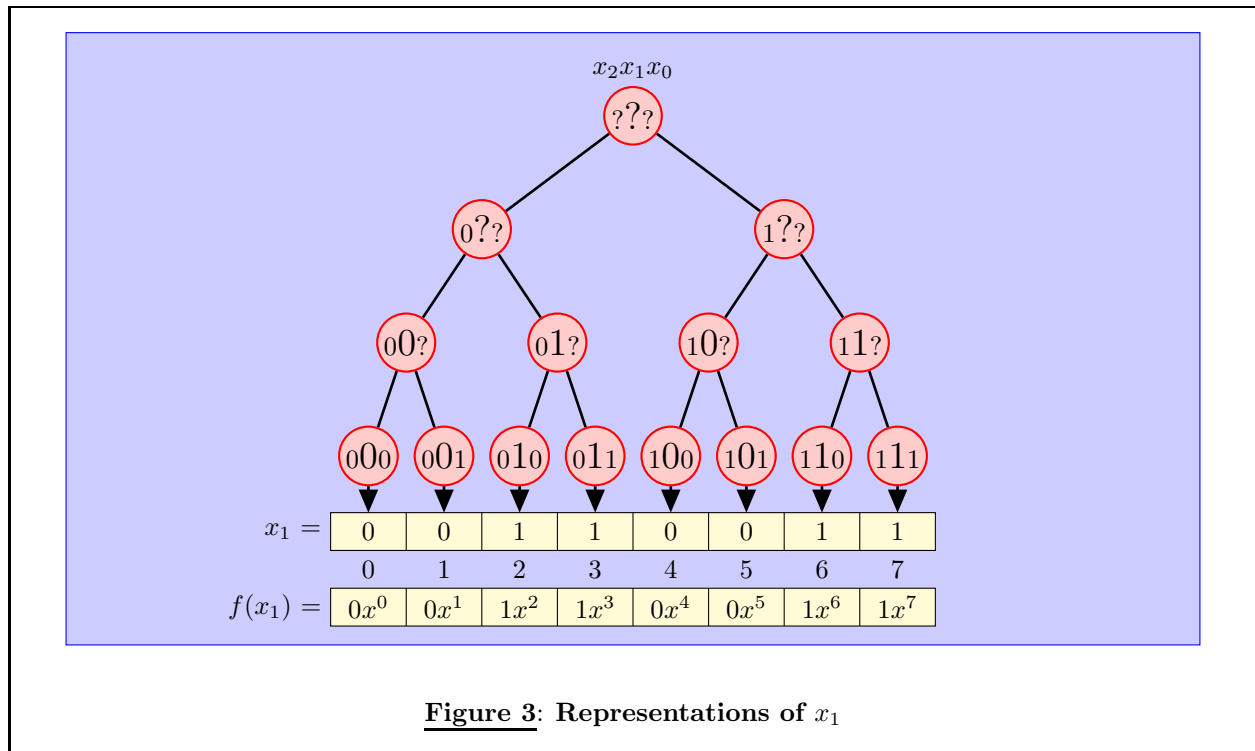
Conventional SAT and k -SAT solvers function by learning clauses or making random guesses at solu-

tions ([14] and the recent survey [15]).

The current best upper bounds for 3-SAT is $O(1.32113^n)$ time, and can be found in ISAAC 2010 by Iwama et al[16]. There's an arXived paper by Hertli, Moser and Scheder which gives an $O(1.321^n)$ time algorithm[17]. These are all randomized algorithms. There is an arXived, deterministic 3-SAT algorithm by Kutzkov and Scheder that runs in time $O(1.439^n)$ [18].

There is a paper that proposed a polynomial runtime for a SAT variant. V.F. Romanov proposed a 3-SAT algorithm that uses "discordant structures", or set-like operations on a lattice, to represent information and determine solutions in polynomial time[19]. However, Liao presents an argument that P is not equal to NP , using a 3-SAT variant, in [9].

Perhaps Baker, Gill, and Solovay's theory of relativization helps explain why there are not more algorithms that attempt to solve NP -complete problems in polynomial time[20]. Their paper "Relativizations of the $P \neq NP$ Question" states that consulting an oracle can lead to situations in which $P \neq NP$.



2 Data Structure(s)

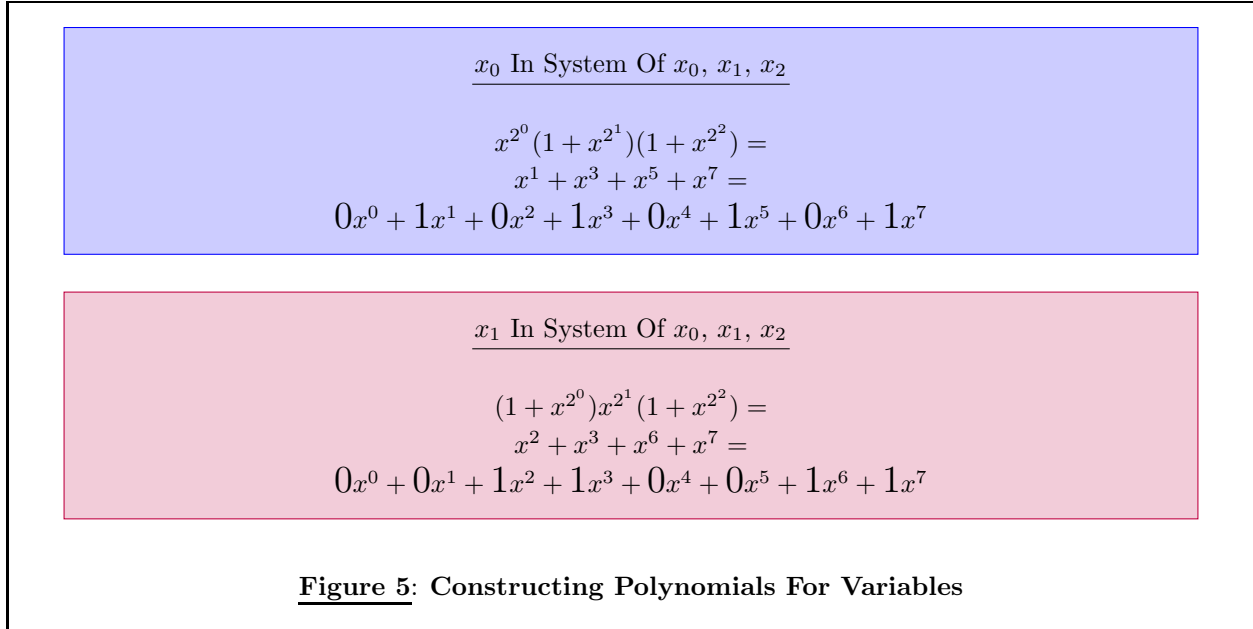
One of the most fundamental components of the algorithm will be referred to as the *clause polynomial*. Figure 3 shows the basic organization of clause polynomials. Essentially, the complete information of one clause is represented by a polynomial of one variable. That is, for each particular truth assignment of all variables, the polynomial “records” whether the clause satisfies this assignment. This is then attached to the polynomial’s variable, which orders the truth assignments.

Note that the particular truth assignments are shown in red. In this fashion, the same tree that organizes the variables can be repeatedly used, and therefore provides some standard organization to the information. Again, this tree organizes all possible variable assignments. It does so by starting at the root, and then proceeds through all Boolean variables in order, and assigns one node to each possible assignment of true or false for each variable. The leaves (at the bottom) thus represent a complete truth assignment for all variables.

The clause polynomial for a single variable is equivalent to a digit in a binary number. In order to understand this, Figure 4 shows binary numbers composed of one to three bits. The tree in Figure 3 uses a three bit example, since there are three variables; thus one

1 Bit	2 Bits	3 Bits
0(0)	00(0)	000(0)
1(1)	01(1)	001(1)
	10(2)	010(2)
	11(3)	011(3)
		100(4)
		101(5)
		110(6)
		111(7)

Figure 4: Binary Representations



bit for each variable. Note then, that the middle variable, x_1 , out of x_0 , x_1 , and x_2 , corresponds with the middle bit. This can be seen in the figure by looking at the middle bit for each binary representation of three bits (which is displayed larger than the other two bits). The sequence is the same as the binary tree above.

2.1 Constructing Clause Polynomials

A basic clause is of the form

$$x_{a_0} \vee x_{a_1} \vee \cdots \vee x_{a_s} \quad (2.1)$$

The algorithm seeks to construct clause polynomials for clauses in this form. This is a two step process. The basic theory behind the process is fairly easily explained here, although the technicalities and a proof are saved for Appendix A on page 26.

To begin to understand how clause polynomials are constructed, a few patterns are observed. Figure 6, on the next page, helps to demonstrate these. First, the obvious pattern of binary digits appears for the variables on the lefthand side. All variables have a pattern of 2^i zeros and then 2^i ones for variable x_i , which then repeats. These variables, in conjunction, correspond with binary numbers. In other words, for the least significant bit, the pattern is zero, then one, and then it repeats. For the next least significant bit (or variable), the pattern has two zeros and then two ones, which then repeats. This pattern continues for all variables.

Observing this pattern, an easy way to construct the clause polynomials for a single variable becomes clear. In fact, it can be summarized as a simple formula:

$$f(x_m) = \left(\prod_{k=0}^{m-1} (1 + x^{2^k}) \right) x^{2^m} \left(\prod_{k=m+1}^n (1 + x^{2^k}) \right) \quad (2.2)$$

Here $\prod (f(x))$ denotes the (indefinite) product of a function of x . More information can be found about indefinite products in [26]. This is taken over a system of $n + 1$ variables.

Figure 5 shows how the clause polynomials are actually constructed using the formula. Note that these are all for a single variable. For the x_0 example, $m = 0$ since the variable is x_0 . In other words, if the variable was x_{32} , then the algorithm would plug in $m = 32$ into the formula. Note, then, that n is one less than the total number of variables, so in both cases it is two, since there are three variables. Returning to the x_0 example, the lefthand product has nothing inside it, the middle follows from knowing n , and the right side product is determined from m and n and the rules of products. For the x_1 example, there is a product on the left side to work with, since m is now one, and k is set to zero for this. Then it follows that $(1 + x^{2^k}) = (1 + x^1)$ since $k = 0$. The right side follows similarly, this time with $k = 2$.

Returning attention to Figure 6 on the previous page, a second pattern can be observed. This is apparent in the blue portion of the figure. Here,

x_4	x_3	x_2	x_1	x_0	$x_1 \vee x_3$	$x_0 \vee x_3$	$x_0 \vee x_2$	$x_0 \vee x_1$	$x_0 \vee x_1 \vee x_3$	$x_0 \vee x_1 \vee x_2$
0	0	0	0	0	0	0	0	0	0	0
0	0	0	0	1	0	1	1	1	1	1
0	0	0	1	0	1	0	0	1	1	1
0	0	0	1	1	1	1	1	1	1	1
0	0	1	0	0	0	0	1	0	0	0
0	0	1	0	1	0	1	1	1	1	1
0	0	1	1	0	1	0	1	1	1	1
0	0	1	1	1	1	1	1	1	1	1
0	1	0	0	0	1	1	0	0	0	0
0	1	0	0	1	1	1	1	1	1	1
0	1	0	1	0	1	1	0	1	1	1
0	1	0	1	1	1	1	1	1	1	1
0	1	1	0	0	1	1	1	0	0	0
0	1	1	0	1	1	1	1	1	1	1
0	1	1	1	0	1	1	1	1	1	1
0	1	1	1	1	1	1	1	1	1	1
1	0	0	0	0	0	0	0	0	0	0
1	0	0	0	1	0	1	1	1	1	1
1	0	0	1	0	1	0	0	1	1	1
1	0	0	1	1	1	1	1	1	1	1
1	0	1	0	0	0	0	1	0	0	0
1	0	1	0	1	0	1	1	1	1	1
1	0	1	1	0	1	0	1	1	1	1
1	0	1	1	1	1	1	1	1	1	1
1	1	0	0	0	1	1	0	0	0	0
1	1	0	0	1	1	1	1	1	1	1
1	1	0	1	0	1	1	0	1	1	1
1	1	0	1	1	1	1	1	1	1	1
1	1	1	0	0	1	1	1	0	0	0
1	1	1	0	1	1	1	1	1	1	1
1	1	1	1	0	1	1	1	1	1	1
1	1	1	1	1	1	1	1	1	1	1

Figure 6: Repeating Patterns of Clauses

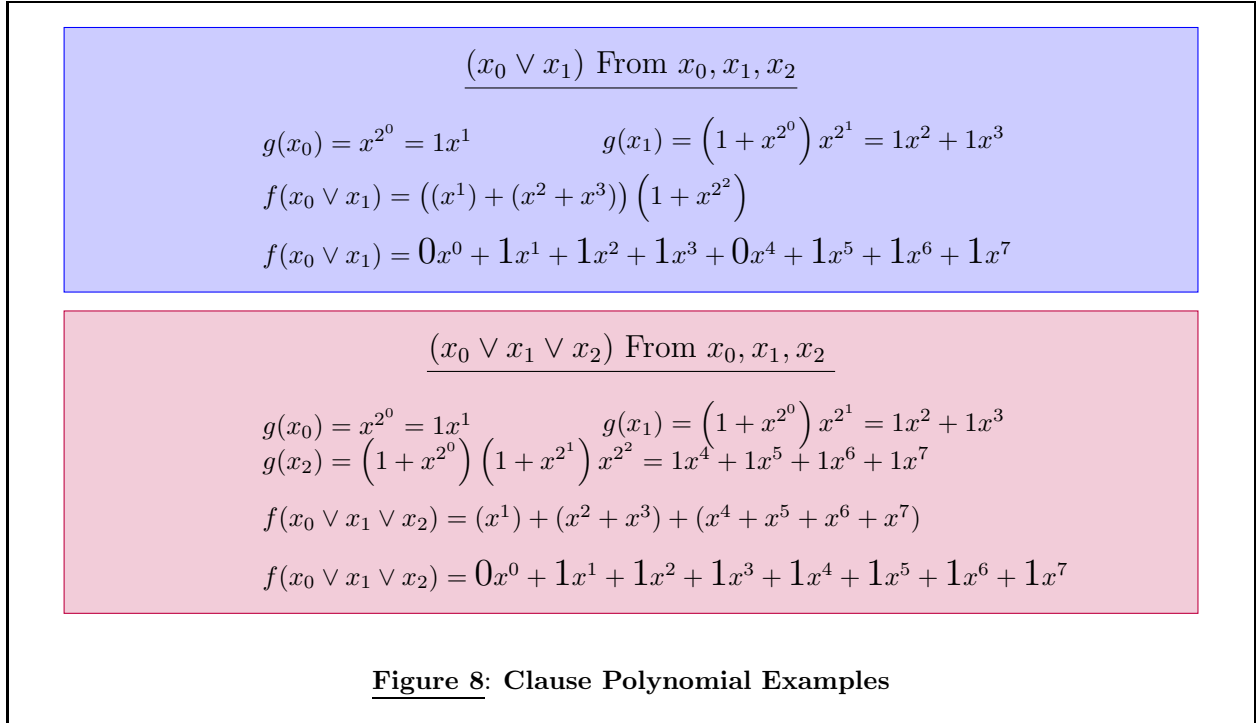
For Clauses of the Form $x_{a_0} \vee x_{a_1} \vee \cdots \vee x_{a_z}$

```

FOR EACH  $x_{a_i}$ 
  CALCULATE  $g(x_{a_i}) = \left( \prod_{k=0}^{a_i-1} (1 + x^{2^k}) \right) x^{2^{a_i}}$ 
LET Result = 0
FOR  $h = 0$  TO  $z$ 
  IF  $(h = a_i)$  FOR SOME  $a_i$ 
    Result = Result +  $g(x_h)$ 
  ELSE
    Result = Result ·  $(1 + x^{2^h})$ 
RETURN Result

```

Figure 7: Clause Polynomial Construction Algorithm



the second pattern is shown in boxes for two-variable clauses. There is the original one-variable pattern of ones and zeros, which is then followed by a series of ones. Note that the series of ones is exactly the same size as the original single-variable pattern. This entire pattern then repeats.

The observed pattern comes from the combination of two variables. The long series of ones comes from the variable that is “larger” than the other. The short series of repeating ones and zeros comes from the “smaller” of the two variables. Together, they form a series that repeats. Another way of looking at it is that both variables form a repeating series, and combining these two repeating series creates another repeating series.

In fact, the pattern of repetition continues even as more variables are added to the clause. The purple portion of the figure shows the repetition(s) involved with three variables. Again, combining two variables produces a short, repeating series. When a third variable (that is strictly “larger” than the other two) is added, a longer, yet repeating, series emerges.

Again, the technicalities of all of this are presented (and solved) in Appendix A on page 26.

There is a very simple algorithm to calculate clause polynomials for any amount of variables, as long as they are in the form given in Equation 2.1. Figure 7 shows the algorithm. The basic idea is to first calculate the the (possibly long) sequence of ones that

repeats for each variable. This is then shifted into the proper position. It is identical to the clause calculations for one variable, with the exception that the series is not made to repeat. The idea is that using “smaller” variables, the algorithm will construct short repeating sequences, and add in the appropriate larger variable when the repeating sequence gets large enough. So essentially, it constructs one large repeating sequence by making the smaller variable sequences repeat, and adding in larger variables when the sequence gets large enough.

Figure 8 shows examples of creating clause polynomials for given problems. Note that the complete set of variables for the original problem must be known ahead of time, just as for clauses of individual variables. As can be seen, the results from this figure correspond with the first eight values from the corresponding clauses in Figure 6.

There is really only one operation remaining to being able to construct essentially any clause polynomial of the form in Equation 2.1; negation. As it turns out, negation is not much more difficult than constructing non-negated clause polynomials.

x_4	x_3	x_2	x_1	x_0	$\overline{x_0}$	$\overline{x_0} \vee x_1$	$x_0 \vee x_1$	$x_0 \vee \overline{x_1}$	$x_0 \vee \overline{x_1} \vee x_2$	$x_0 \vee \overline{x_1} \vee \overline{x_2}$
0	0	0	0	0	1	1	0	1	1	1
0	0	0	0	1	0	0	1	1	1	1
0	0	0	1	0	1	1	1	0	1	1
0	0	0	1	1	0	1	1	1	1	1
0	0	1	0	0	1	1	0	1	1	1
0	0	1	0	1	0	0	1	1	1	1
0	0	1	1	0	1	1	1	0	1	1
0	0	1	1	1	0	1	1	1	1	1
0	1	0	0	0	1	1	0	1	1	1
0	1	0	0	1	0	0	1	1	1	1
0	1	0	1	0	1	1	1	0	1	1
0	1	0	1	1	0	1	1	1	1	1
0	1	1	0	0	1	1	0	1	1	1
0	1	1	0	1	0	0	1	1	1	1
0	1	1	1	0	1	1	1	0	1	1
0	1	1	1	1	0	1	1	1	1	1
1	0	0	0	0	1	1	0	1	1	1
1	0	0	0	1	0	0	1	1	1	1
1	0	0	1	0	1	1	1	0	0	1
1	0	0	1	1	0	1	1	1	1	1
1	0	1	0	0	1	1	0	1	1	1
1	0	1	0	1	0	0	1	1	1	1
1	0	1	1	0	1	1	1	0	1	1
1	0	1	1	1	0	1	1	1	1	1
1	1	0	0	0	1	1	0	1	1	1
1	1	0	0	1	0	0	1	1	1	1
1	1	0	1	0	1	1	1	0	0	1
1	1	0	1	1	0	1	1	1	1	1
1	1	1	0	0	1	1	0	1	1	1
1	1	1	0	1	0	0	1	1	1	1
1	1	1	1	0	1	1	1	0	1	1
1	1	1	1	1	0	1	1	1	1	1

Figure 9: Patterns of Clauses With Negation

For Clauses of the Form $x_{a_0} \vee x_{a_1} \vee \dots \vee x_{a_z}$

```

 $g(\overline{x_{a_i}}) = \left( \prod_{k=0}^{a_i-1} (1 + x^{2^k}) \right)$ 
...
IF ( $h = \overline{a_i}$ ) FOR SOME  $\overline{a_i}$ 
    Result = Result  $\cdot$  ( $x^{2^{a_i}}$ ) +  $g(\overline{x_{a_i}})$ 
ELSE IF ( $h = a_i$ ) FOR SOME  $a_i$ 
    Result = Result +  $g(x_h)$ 
ELSE
    Result = Result  $\cdot$  ( $1 + x^{2^h}$ )
...

```

Figure 10: Negated Clause Polynomial Construction Algorithm

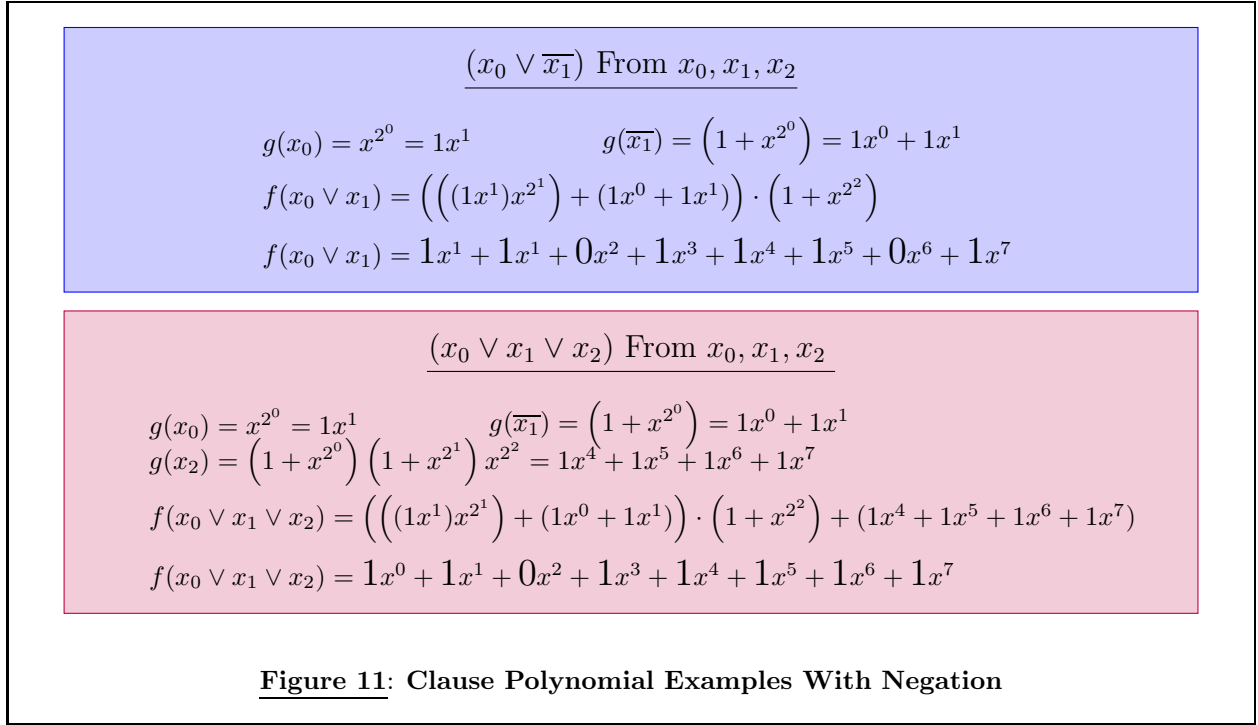


Figure 9, on the previous page, displays clause patterns with negated variables. As can be noted by the negated variable x_0 near the left, it is just a reversed version of ones and zeros, compared to the non-negated x_0 displayed just to the left of it. In other words, just as negation reverses true and false values in Boolean algebra, negation reverses zeros and ones in clause polynomials. In fact, this is how all single-variable clauses are negated; simply swap the zeros and ones. There is actually a very simple and effective way to do this - the negated clauses are the same as the regular clauses except for the fact that they are not multiplied by a power of x^{2^m} , as the regular clauses are. This is the equivalent as removing this term from Equation 2.2, hence the resulting equation:

$$f(\overline{x_m}) = \left(\prod_{k=0}^{m-1} (1 + x^{2^k}) \right) \left(\prod_{k=m+1}^n (1 + x^{2^k}) \right) \quad (2.3)$$

Again, this is for a system of $n+1$ variables, and n can be adjusted accordingly for the size of the problem.

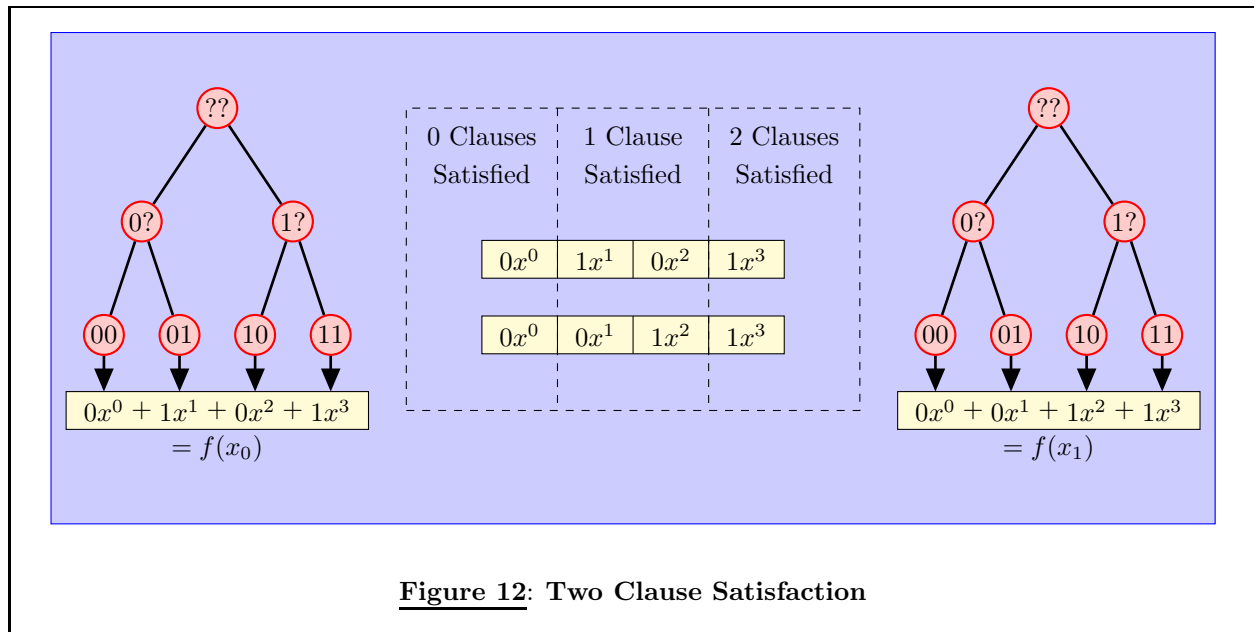
Next, attention can be turned to the new patterns observed for multiple-variable clauses. Figure 9 shows the negated values of $\overline{x_0}$ next to the combined clause $\overline{x_0} \vee x_1$. Note that the pattern of ones coming from x_1 has not changed in any way; however,

the repeating pattern of zeros and ones coming from $\overline{x_0}$ has been switched, compared to the non-negated equation $x_0 \vee x_1$ beside it on the right. So really, it is becoming evident that negating variables only swaps the pattern of ones that the variable creates.

This is more evident if the clause $x_0 \vee \overline{x_1}$ is observed beside it. Here the pattern of ones coming from the variable x_1 has changed, since x_1 has been negated. So again, there is evidence that the pattern of ones coming from a variable is simply “exchanged” or placed elsewhere. It can be seen, though, that this does not change the pattern for x_2 , as evidenced in the equation $x_0 \vee \overline{x_1} \vee x_2$ beside it.

Finally, it’s seen that swapping the pattern of ones may entail moving a smaller group of ones and zeros. This is evidenced in the final clause in the figure. Here, the variable x_2 has been negated, which causes a shift in the largest pattern of ones, which is due to x_2 .

Two examples have been worked out in slight detail in Figure 11. Here the pattern is mostly the same, with the exception that negating variables causes some values to be swapped. This is the equivalent of moving the pattern of ones. The adjustments to the algorithm are shown in Figure 10 on the previous page.



3 Two Clause Problems

Now that sufficient background has been presented, the major ideas behind the algorithm can be introduced. Two clause problems are some of the simplest cases, yet they allow the fundamental ideas to be introduced and studied.

Figure 12 shows the four basic possible combinations between two clauses. If a clause polynomial is considered with any amount of terms (powers of x), there are only two possible values (known in mathematics as coefficients) that can be associated with each term; zero or one. If two clauses are considered, there are two possible values for the coefficient of the first polynomial, and two possible values for the coefficient of the second polynomial, for a total of four different combinations.

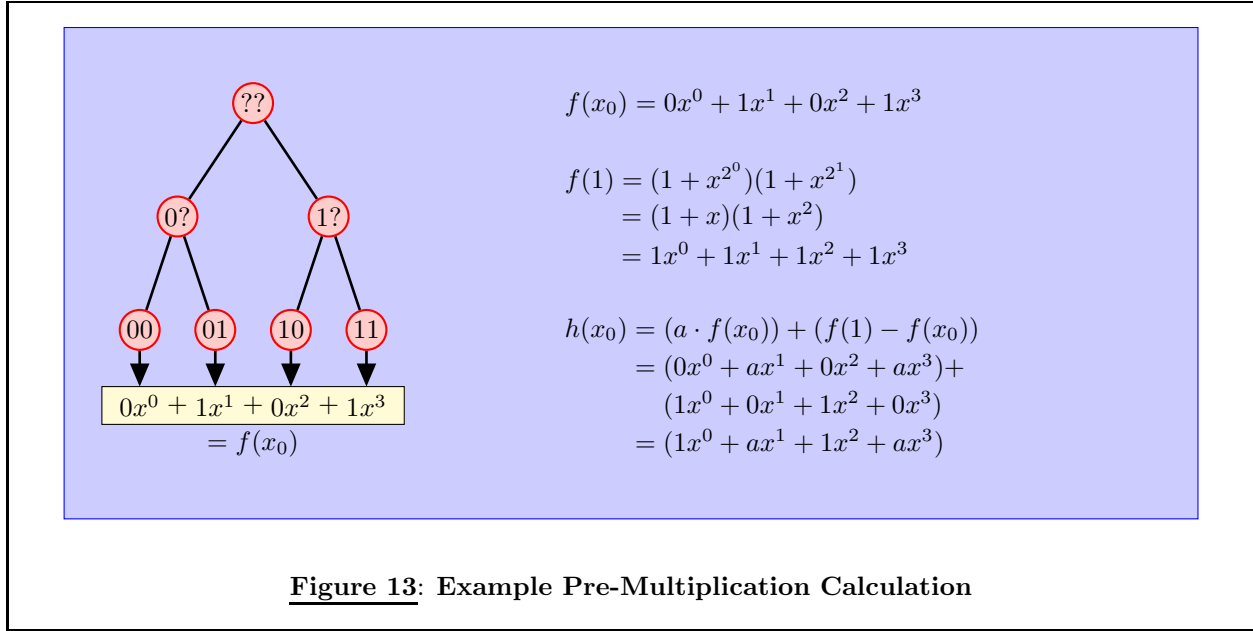
The figure shows two clause polynomials and the trees associated with them. In the middle, the four possible combinations can be seen. Remembering that the coefficients represent satisfaction for a particular truth assignment, it's possible to note the total satisfaction for two clauses considered simultaneously. When both clauses have a zero coefficient, that indicates that neither clause will satisfy the original question of satisfaction for that particular truth assignment. Looking through the clause trees, it's seen that this assignment corresponds to $(x_0 = \text{false}, x_1 = \text{false})$. So this truth assignment won't satisfy any of the clauses. On the other hand, the two truth assignments in the middle of the figure each satisfy one clause. The truth assignment

$(x_0 = \text{true}, x_1 = \text{true})$ is seen to satisfy both clauses, and so it is a solution to the original problem. Again, the reason it satisfies both clauses is that it has a one for both coefficients, thus signifying that both clauses are satisfied.

One important thing to note here is that between two clauses, there are really only three possible satisfaction results. Either zero, one, or both of the clauses are satisfied (for any particular truth assignment). One general idea that, although perhaps trivial, will be important is that there are really only three types of satisfaction between two clauses. This basic concept will be extended to see that there are really only $n+1$ possible types of satisfaction between n clauses.

The fundamental idea here is that the problems can be simplified so that large problems can really be dealt with by simply considering the types of satisfaction, which are fairly simple. For two clause problems, it will really only be necessary to deal with the three types of satisfaction, and interactions between the different types of satisfaction.

It will be shown how operations of multiplication and addition can be used to work with the three different types of satisfaction, and to solve questions about them. This will be essentially simpler and in some ways necessary to overcome the complications of working with all of the possibilities between two or more clauses.



3.1 Manipulating Clause Polynomials

In order to simplify clause calculations into the equivalence classes of satisfaction, it is necessary to modify the original clause polynomials.

The first modification used is a simple one. The algorithm will need to change all of the coefficients that are equal to one into coefficients that are equal to a . This is easy; it is just multiplication by a . Here's an example:

$$f(x) = 0x^0 + 1x^1 + 0x^2 + 1x^3$$

$$a \cdot f(x) = 0x^0 + ax^1 + 0x^2 + ax^3$$

The next modification is a bit tougher; it is exchanging the one and zero coefficients. This can be done by subtracting the original function from a function of ones. This inverts the bits, since the ones are subtracted from ones to become zeros, and the zeros are subtracted from ones to become ones. However, the function of all ones is needed. This function is, for a system of V variables:

$$f(1) = \prod_{k=0}^{V-1} (1 + x^{2^k}) \quad (3.1)$$

Note that:

$$f(1) = 1x^0 + 1x^2 + 1x^3 + \dots + 1x^{2^V-1}$$

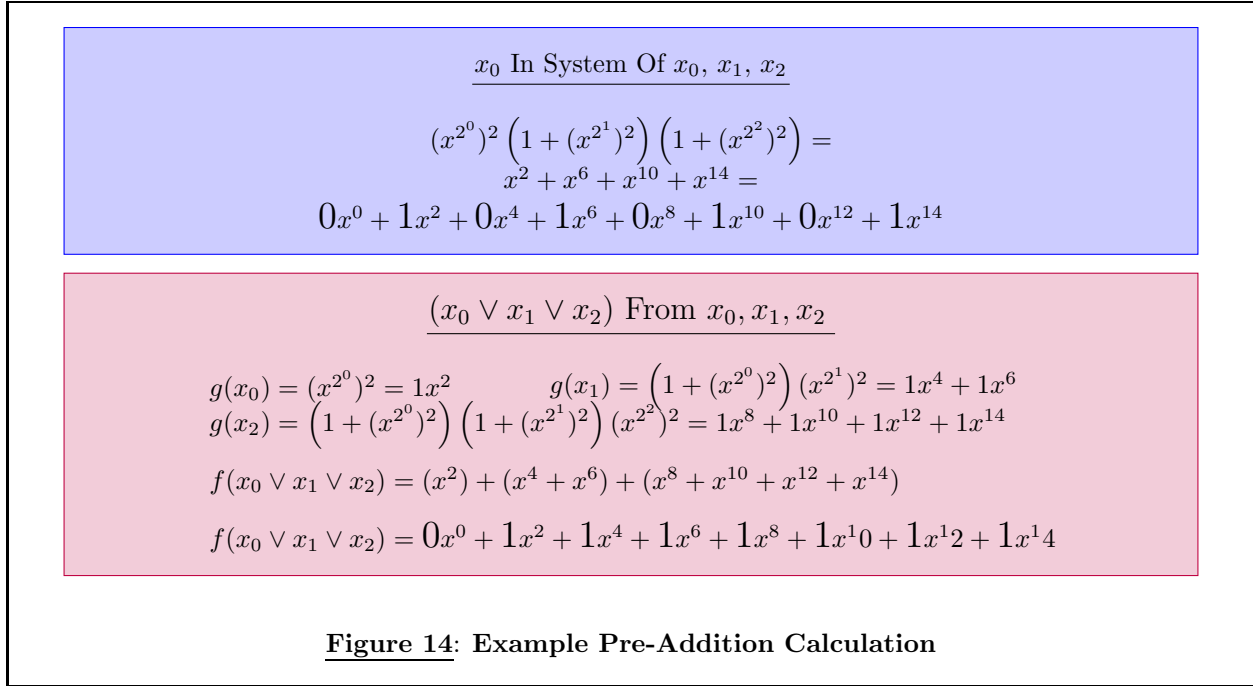
This completes the requirements for multiplication. The algorithm uses this knowledge to change the one

coefficients into a coefficients and the zero coefficients into one coefficients. Then multiplication can be performed, as will be seen.

Figure 13 exhibits the steps taken before a function is ready for multiplication. $f(x_0)$ is given through a tree, before multiplication. The ones must be transformed into as , and the zeros must be transformed into ones. Note the final result, $h(x_0)$. It is the finished calculation, ready for multiplication.

To do this, the function of ones for a two-variable system must be calculated. Then the original function can be multiplied by a to transform the one coefficients, and it is also subtracted from the function of ones (seperately) to transform the zero coefficients. These are added together for the final result.

Note that this procedure works for any clause in any system with any amount of variables. It simply prepares the clause polynomials for special processing, or interactions, with other clause polynomials. This may not seem like much, but it greatly simplifies the system.



Addition requires modifications too. However, these modifications are of a different variety than those of multiplication. Essentially, the power of x needs to be doubled.

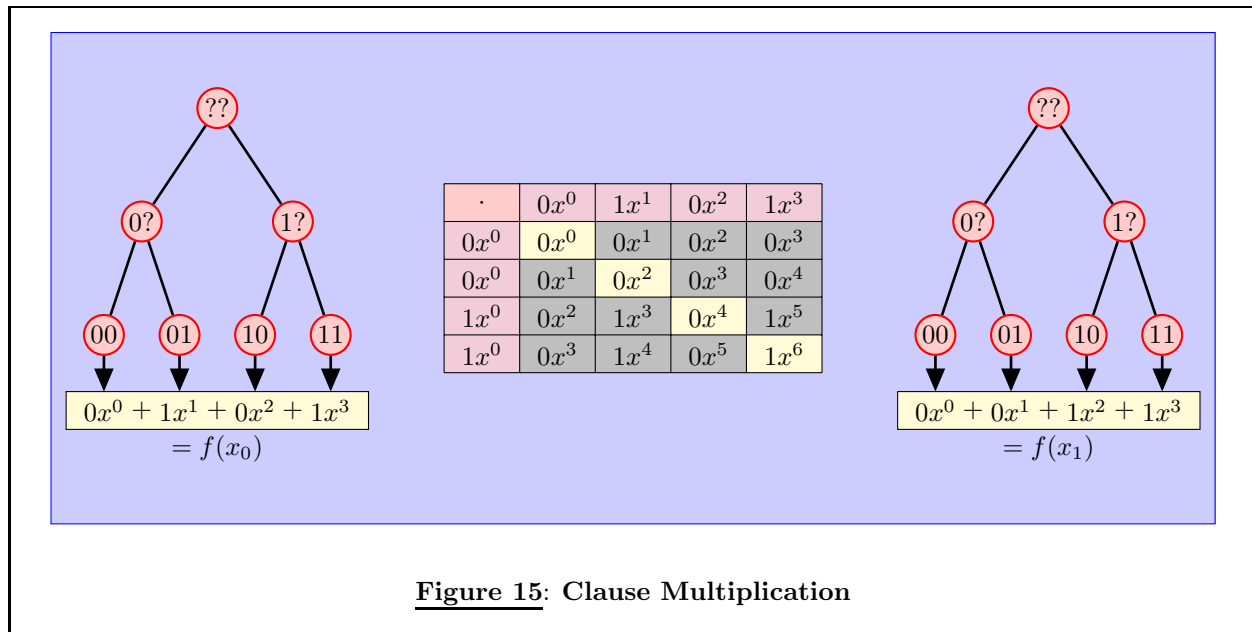
Doubling the power of x can actually be fairly simple. Figure 14 displays a redo of the creation of clause polynomials. The first part of the example is really just Figure 5 on page 5, modified for doubling the power of x . Note that each power of x , once it is essentially calculated, is doubled. The result is that all of the powers of x are multiplied by two in the finished clause polynomial.

The second part of the figure is also a redo, this time of a multiple variable clause taken from Figure 8 on page 7. Again, the main idea is that the powers of the variable x is doubled.

The actual operation of addition is also performed on one special value, which comes in part from the ideas of multiplication. A constant is added to each coefficient of the polynomials. This constant is the same value for all coefficients, so the function of ones once again becomes useful. Unfortunately, in its originally derived form, the powers of x are not the same as the powers of x used in addition. So once again, the same principles are used to double the powers of x for the function of ones. It is really as simple to do this as altering every power of x in the original equation (Equation B on page 26). The new formula for the modified function of ones is as follows:

$$f(1modified) = \prod_{k=0}^{V-1} (1 + (x^{2^k})^2) \quad (3.2)$$

These operations will be very useful in the material ahead.



\wedge	False	True
False	False	False
True	False	True

\cdot	0	1
0	0	0
1	0	1

Figure 16: Operation Equivalence

logical operation of conjunction (\wedge) and the arithmetic operation of multiplication (\cdot) are equivalent on bit values. So it's not totally unpredictable that multiplication of a clause polynomial contains results similar to conjunction. The diagonal in Figure 15 contains like terms multiplied by like terms. Only the coefficients (or numbers attached to the terms) may differ. The result (along the diagonal) is known in mathematics as the Hadamard product, and the algorithm is concentrated on separating this diagonal term from the off-diagonal terms.

3.2 Multiplication

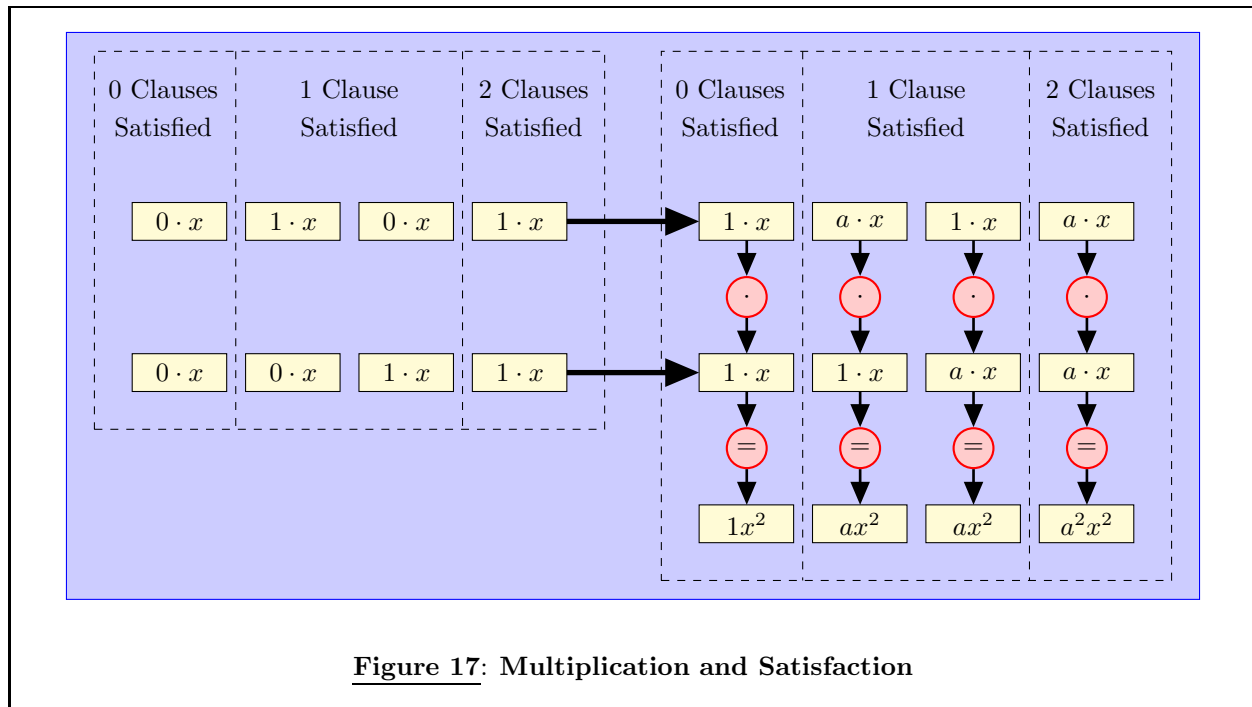
It could be said that the algorithm is focused around (arithmetic) multiplication of clause polynomials.

Figure 15 details an example. It begins with two clause polynomials, $f(x_0)$ and $f(x_1)$. The associated trees are shown that go with the clause polynomials. In the middle, the clause polynomials are broken into pieces and multiplied piecewise. Every part of each polynomial is multiplied with every part of the other polynomial. This corresponds with plain old arithmetic multiplication of two polynomials. However, an interesting event happens here. The result that lies along the diagonal (shown in yellow) corresponds with the result $f(x_0 \wedge x_1)$. That is, the diagonal represents the corresponding clause polynomial for the result of conjunction. The idea here is that multiplication of clause polynomials can be used to evaluate the original Boolean equation.

Figure 16 helps give a partial explanation of why this occurs. As can be seen from the truth tables, the

The reason why the algorithm is so closely associated with the Hadamard product, or the diagonal terms, is that it is essentially the solution to the original problem. Since it tells which terms are satisfying, the algorithm can simply count the number of satisfying terms along the diagonal. If there are any satisfying terms, then the original problem can be satisfied. Otherwise, it can't be satisfied.

So at this point in the ideology, the original Boolean problem has been transformed from a question about Boolean arithmetic, to a question concerning how to get information about the diagonal (or Hadamard product).



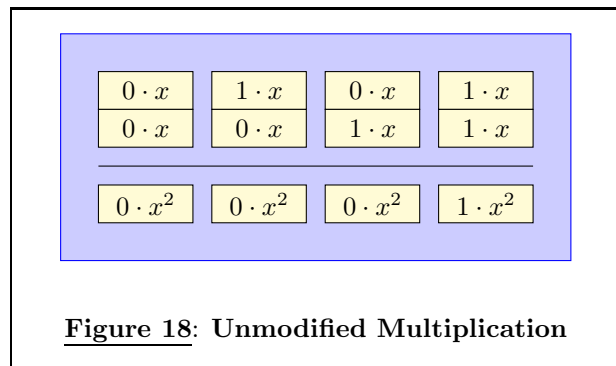
3.3 Multiplication and Satisfaction

Figure 17 shows another viewpoint of arithmetic multiplication. This time the four different cases based on the coefficients are shown. In other words, between any two coefficients being multiplied, the input coefficients must be one of four cases. Also, on the left, the satisfaction between the two original coefficients is shown. Then, on the right, the corresponding modified coefficients and their results are shown. Note that there are still really three cases of satisfaction, resulting in $1x^2$, ax^2 , and a^2x^2 .

It's seen that modifying the coefficients for multiplication has allowed for the three cases to appear in the results of multiplication. This is one of the keys to getting things to work correctly. The algorithm is really interested in the case when both clauses are satisfied.

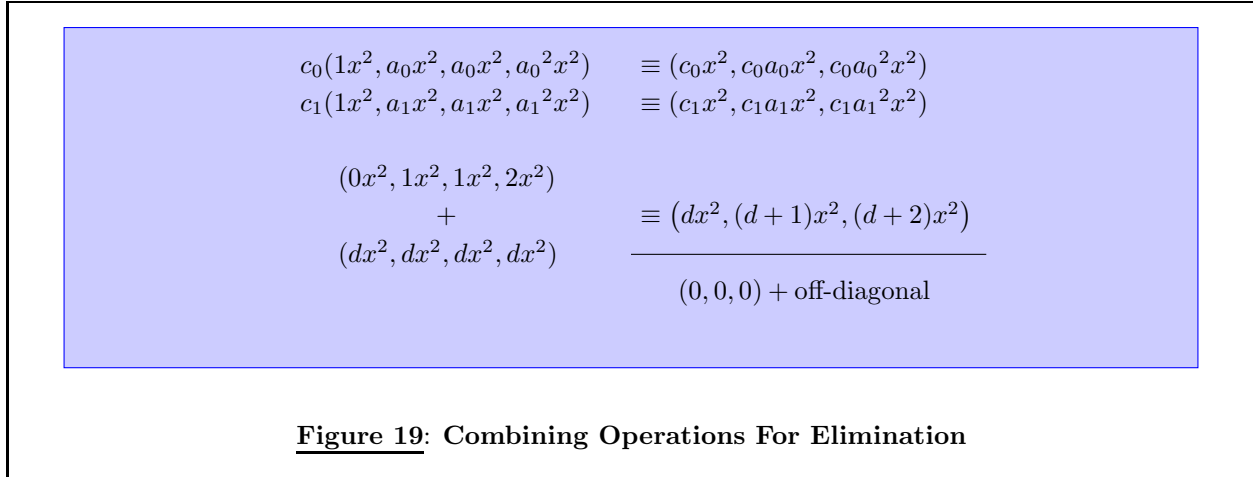
Unfortunately, the results for multiplication mix the diagonal and off-diagonal cases together. In order to isolate the diagonal, there will be some tricky interplay between multiplication and addition ahead.

One thing that can be noted is that multiplication with the original clause polynomials isolates the case where everything is maximally satisfied (both clauses are satisfied). This can be seen in Figure 18. Note that only the case on the far right (where both clauses have nonzero coefficients) returns anything other than zero. Now this will occur for both



diagonal and off-diagonal values, but it's very close to a solution. The algorithm wants the diagonal portion of this result, and seeks to somehow eliminate the off-diagonal portion of it.

The next subsection will show how the algorithm can begin to separate diagonal terms from off-diagonal terms. The algorithm's efforts will be concentrated on separating diagonal values from off-diagonal values, since the result will lead to a solution.



3.4 Eliminating The Diagonal

Figure 20, on the following page, presents the cases for addition alongside the better-explored operation of multiplication. The main thing to note is that addition can return one of three results, just like the equivalence classes of satisfaction. In fact, they are once again related in the same way that multiplication is related to satisfaction.

Figure 21 shows what is proposed for the algorithm. It will take two multiplication operations (three are shown, but this is more than needed), and combine them with one addition, to eliminate everything except for the off-diagonal values, which are shown as gray triangles.

Everything is really summarized as arithmetic in Figure 19. Here, the original results are shown on the left, being modified so that they can be combined together. It can be noted that the middle two cases have always had equal results, so they have been combined. *The right side shows only three cases in parenthesis, which are the satisfaction equivalences.* The algorithm seeks to eliminate these, thus the sums at the bottom are zero, except for the off-diagonal.

Here the algorithm comes up with three equations that must be satisfied:

$$c_0 + c_1 - d = 0 \quad (3.3)$$

$$c_0a_0 + c_1a_1 - (d+1) = 0 \quad (3.4)$$

$$c_0a_0^2 + c_1a_1^2 - (d+2) = 0 \quad (3.5)$$

Again, these come from the three cases on the right side of Figure 19, summing the columns.

To summarize all of this again, what is essentially happening is that two multiplications, together with an addition, cancel out all coefficients along the diagonal. However, multiplication creates off-diagonal

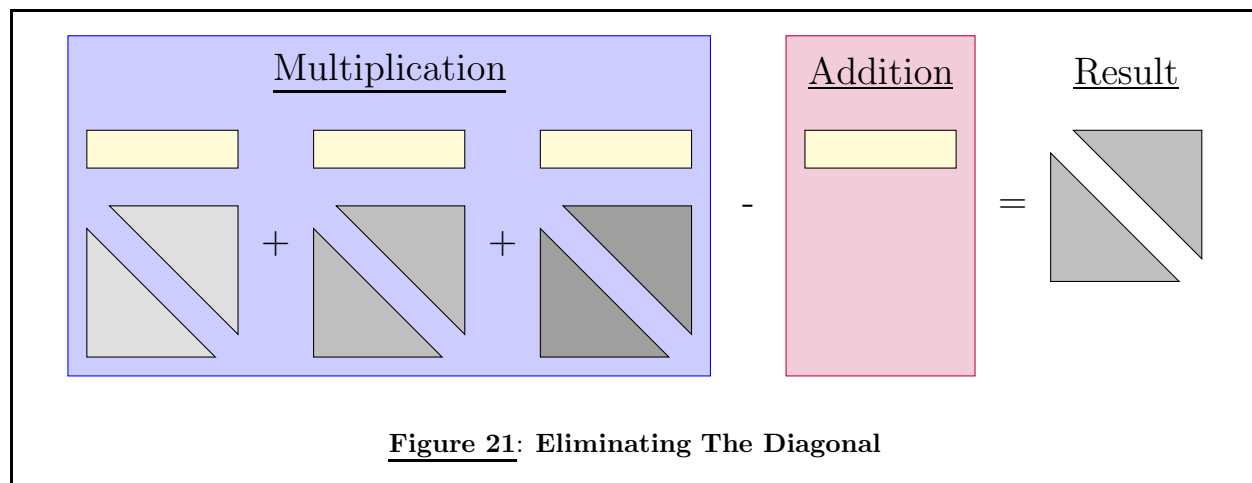
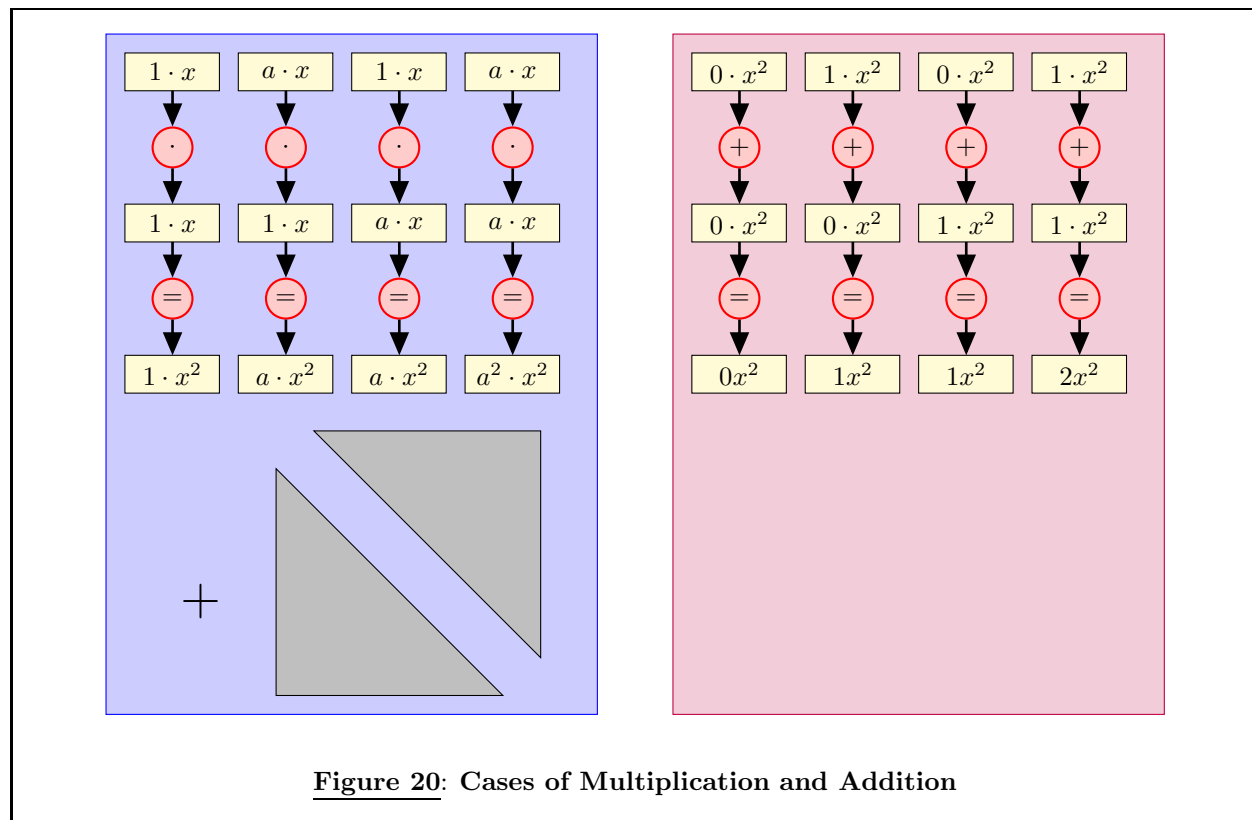
values, and these values will remain. So in effect, the algorithm isolates off-diagonal values. It does so by using the values calculated from addition to cancel out the diagonal from multiplication.

So now the algorithm can concentrate fully on eliminating the terms along the diagonal to isolate the off-diagonal terms. The following subsection will explore how to get these terms to cancel.

First, it's time to introduce modular arithmetic. Subsection C.11 in the Appendix notes some sources that go over modular arithmetic. To simplify the ideas, essentially all calculations are performed as usual, except that an additional operation is performed afterwards. After the calculations are done, to get the result modulo a prime p , the algorithm does the equivalent of taking the remainder after dividing the result by p . Thusly, all calculations are represented by an integer greater than or equal to zero and less than p . So all calculations have a very limited range of values that can result.

This introduces a notion of equivalence, where two values are equivalent if they are the same modulo p . This allows the algorithm to find solutions more easily, since the normal restriction that calculations must be equal is relaxed so that calculations must only be equivalent.

Equivalence is really introduced so that the equations that must be satisfied can be solved. The relaxed restrictions allow for solutions that can be found easily.



$c_0 = 1$	$c_0 = 2$	$c_0 = 3$	$c_0 = 4$
$\begin{array}{l} 1 \equiv 1 \\ a_0 \equiv 2 \\ a_0^2 \equiv 4 \end{array} \left. \begin{array}{l} \} 1 \\ \} 2 \end{array} \right\} 1$	$\begin{array}{l} 2 \cdot 1 \equiv 2 \\ 2 \cdot a_0 \equiv 4 \\ 2 \cdot a_0^2 \equiv 1 \end{array} \left. \begin{array}{l} \} 2 \\ \} 4 \end{array} \right\} 2$	$\begin{array}{l} 3 \cdot 1 \equiv 3 \\ 3 \cdot a_0 \equiv 6 \\ 3 \cdot a_0^2 \equiv 5 \end{array} \left. \begin{array}{l} \} 3 \\ \} 6 \end{array} \right\} 3$	$\begin{array}{l} 4 \cdot 1 \equiv 4 \\ 4 \cdot a_0 \equiv 1 \\ 4 \cdot a_0^2 \equiv 2 \end{array} \left. \begin{array}{l} \} 4 \\ \} 1 \end{array} \right\} 4$
$c_0 = 5$	$c_0 = 6$	$c_0 = 0$	
$\begin{array}{l} 5 \cdot 1 \equiv 5 \\ 5 \cdot a_0 \equiv 3 \\ 5 \cdot a_0^2 \equiv 6 \end{array} \left. \begin{array}{l} \} 5 \\ \} 3 \end{array} \right\} 5$	$\begin{array}{l} 6 \cdot 1 \equiv 6 \\ 6 \cdot a_0 \equiv 5 \\ 6 \cdot a_0^2 \equiv 3 \end{array} \left. \begin{array}{l} \} 6 \\ \} 5 \end{array} \right\} 6$	$\begin{array}{l} 0 \cdot 1 \equiv 0 \\ 0 \cdot a_0 \equiv 0 \\ 0 \cdot a_0^2 \equiv 0 \end{array} \left. \begin{array}{l} \} 0 \\ \} 0 \end{array} \right\} 0$	

Figure 22: Multiplication Results Modulo 7

To find solutions that eliminate the diagonal, a finite field is introduced, allowing operations to be conducted modulo a prime p . Figure 22 displays calculations inside a field modulo 7. Here the algorithm selects $a_0 = 2$, although it could select really any value other than one or zero. It then calculates the results of multiplication (times a constant c_0), which for the various equivalence classes are $c_0 \cdot 1$, $c_0 \cdot a_0$, and $c_0 \cdot a_0^2$.

The algorithm is really interested in the second-order difference. This is illustrated in Figure 23. That is, it takes the difference between results, and then takes the difference of these differences.

It's fairly straightforward to get the initial results; using arithmetic multiplication works fine. Then the results have to be modulated. As an example, in Figure 23, a_1 is set as three. Then, to calculate a_1^2 , take $3^2 = 9$. Then $9/2 = 1$ with remainder 2. So the result is the remainder, which is 2.

That gets the initial results, in the field. Then to get the first order differences, take successive results and subtract the first from the successive. This is illustrated very clearly in the figure, which does a better job of explaining. The take the difference again, which is called the second-order difference.

The reason that it's so important to get these second-order differences is that they help match up multiplication results. Note that both figures are actually two separate multiplications; Figure 22 uses a_0 and c_0 while Figure 23 uses a_1 and c_1 . They both use the same prime, so they are two separate multiplication results that can be matched up. The goal is to

$$\begin{array}{l} 1 \equiv 1 \pmod{7} \\ a_1 \equiv 3 \pmod{7} \\ a_1^2 \equiv 2 \pmod{7} \end{array} \left. \begin{array}{l} \} 3 - 1 \equiv 2 \\ \} 2 - 3 \equiv 6 \end{array} \right\} 6 - 2 \equiv 4$$

Figure 23: Differences of Multiplication Results

find the second-order differences that add up to zero mod p . Note that the example with a_1 has a second-order difference of four. $3 + 4 = 7 \equiv 0 \pmod{7}$, so the idea is to find a second-order difference of three in the other equation. It is done with $c_0 = 3$. So now two equations have been found that match up.

To check this result, the equations can be combined:

$$\begin{array}{ll} c_0 \cdot 1 + c_1 \cdot 1 \equiv 3 \cdot 1 + 1 \cdot 1 & \equiv 4 \equiv d + 0e \\ c_0 \cdot a_0 + c_1 \cdot a_1 \equiv 3 \cdot 2 + 1 \cdot 3 & \equiv 2 \equiv d + 1e \\ c_0 \cdot a_0^2 + c_1 \cdot a_1^2 \equiv 3 \cdot 4 + 1 \cdot 2 & \equiv 0 \equiv d + 2e \end{array}$$

The main thing to note is that the sequence of results in the equations (4, 2, 0) can be recreated by an addition operation (on clause polynomials). That is, the first equation = $4 + 0(-2)$, the second = $4 + 1(-2)$, and the third = $4 + 2(-2)$.

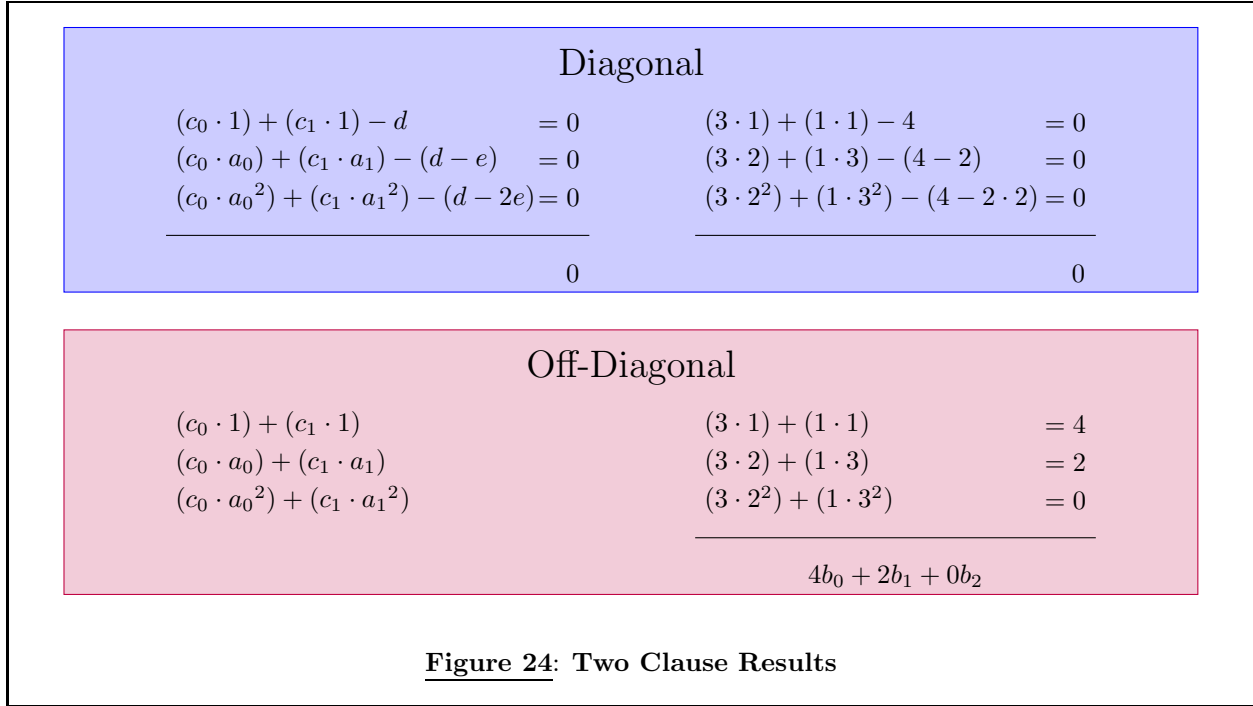


Figure 24 shows the results of combining equations (addition and multiplication). Here the results of clause operations (multiplication and addition) are combined, and are shown according to whether or not they lie along the diagonal. As mentioned previously, the addition operation cancels out the multiplication along the diagonal. However, the results off the diagonal are not cancelled.

Thusly, the results off the diagonal become multipliers for unknown quantities. This is because the polynomials that underline the equations are also part of this mix, and the resulting polynomial quantities are unknown, even though the multipliers are known. Thus these quantities are represented as b_0 , b_1 , and b_2 .

This allows for a new result. Remember that the original quantities are combined together in the previous equations that were used. Thus, this new result represents a sum of the new quantities, along with their respective multipliers. Therefore, the algorithm arrives at a new result which is a single equation in three unknowns.

Again, time for some ideas. Back in Section 3.3 on page 14, Figure 18 is discussed. Especially important is the fact that the maximally satisfied clauses, both along the diagonal and off the diagonal, can be isolated. In this section it has been shown that equations for off-diagonal values can be obtained. Thinking about off-diagonal values, it is possible to cre-

ate other equations using multiplication and addition - and these equations can help determine the off-diagonal values by combining them with the first equation and then using linear algebra to determine the values.

So essentially, the algorithm will use multiplication and addition of modified clause polynomials to create equations in three unknowns. These unknowns are the off-diagonal values. Then, the equations created can be combined via linear algebra to determine the off-diagonal values. As mentioned previously, the algorithm can already isolate the maximally satisfied clause values together. Unfortunately, the off-diagonal and diagonal values are combined together. However, since the off-diagonal portion can be determined via linear algebra, the diagonal portion can be isolated from the off-diagonal portion using simple algebra, and the results from linear algebra (which give the off-diagonal portion).

The diagonal value of maximally satisfied clauses is thus determined, and this corresponds to the number of satisfied solutions. Now if this number is nonzero, the whole problem can be satisfied. Otherwise, the original problem can't be satisfied.

4 A Two Clause Walkthrough

In order to help understand the algorithm, this walkthrough will start at the beginning of execution and proceed through as many steps as possible. The initial problem will be given as the equation:

$$(x_0) \wedge (\overline{x_0} \vee x_1) \quad (4.1)$$

One of the first things to do is to determine the modulus. Using a prime greater than $(2n)^2$ should work well, and it's obvious that there are 2 clauses and 2 variables. 17 should suffice, since $17 > (2 \cdot 2)^2$.

Next, a value should be given to x , which will be used to calculate the clauses. There doesn't seem to be any particularly good way to pick, other than using a number greater than one. Three will be used for this example.

Next, the values for the clauses can be calculated. Recalling Equation 2.2 on page 5:

$$f(x_m) = \left(\prod_{k=0}^{m-1} (1 + x^{2^k}) \right) x^{2^m} \left(\prod_{k=m+1}^n (1 + x^{2^k}) \right) \quad (4.2)$$

So,

$$\begin{aligned} f(x_0) &= (1 + x^{2^1}) x^{2^0} \\ &= (1 + x^2) x^1 \\ &= (1 + 3^2) 3^1 \\ &= (10)3 = 30 \equiv 13 \pmod{17} \end{aligned}$$

The second, trickier equation comes from the same subsection. The algorithm to use is in Figure 10 on page 8. This is modified from Figure 7 on page 6. Here,

$$g(\overline{x_0}) = () = 1 \quad (4.3)$$

There is nothing to multiply, so by convention this product will be set equal to one. As for x_1 :

$$\begin{aligned} g(x_1) &= (1 + x^{2^0}) x^{2^1} \\ &= (1 + x^1) x^2 \\ &= (1 + 3^1) 3^2 \\ &= (4)9 = 36 \equiv 2 \pmod{17} \end{aligned}$$

Now, proceeding through the algorithm starting at $h=0$, that results in the case $h = \overline{a_i}$. So the result

becomes $g(\overline{x_0})$, or 1. Now, h is incremented, so $h=1$. This results in the case $h = a_i$. So $g(x_1)$ is added to the result, giving $1 + 2 = 3$. This finishes the algorithm with the result $f(\overline{x_0} \vee x_1) \equiv 3 \pmod{17}$.

At some time, the equations should be set up so that Boolean algebra can eventually lead to an answer. Now is a good time, so the various results for $a_0 = 2$ and c_0 are shown in Figure 25 on the following page. The goal here is to eliminate the diagonal by taking combinations of equations, as explored in the previous section. Observe what happens if another set of equations is created, with $a_1 = 3$ and $c_1 = 1$:

$$\begin{aligned} c_1 \cdot 1 &\equiv 1 \cdot 1 && \equiv 1 \\ c_1 \cdot a_1 &\equiv 1 \cdot 3 && \equiv 3 \\ c_1 \cdot a_1^2 &\equiv 1 \cdot 3^2 && \equiv 9 \end{aligned}$$

Proceeding as in Figure 23 on page 17, the first differences of this equation are $3 - 1 = 2$ and $9 - 3 = 6$. The second difference is $6 - 2 = 4$. Recalling that the second differences should add up to the modulus (17), a second difference of $17 - 4 = 13$ is required. From Figure 25, it can be seen that setting $c_0 = 13$ in the first set of equations gives a second difference of 13. Thus, these two equations can now be combined successfully. To see this, simply use the original values of a and c in each equation and add them together. For example using $a_0 = 2$ and $c_0 = 13$ for the first equation, and $a_1 = 3$ and $c_0 = 1$ for the second equation, this gives results of combining equations:

$$\begin{aligned} c_0 + c_1 &\equiv 13 + 1 && \equiv 14 \\ c_0(a_0) + c_1(a_1) &\equiv 9 + 3 && \equiv 12 \\ c_0(a_0^2) + c_1(a_1^2) &\equiv 1 + 9 && \equiv 10 \end{aligned}$$

Now corresponding addition equations can be constructed by observing:

$$\begin{aligned} 14 &\iff 14 + 0(-2) \\ 12 &\iff 14 + 1(-2) \\ 10 &\iff 14 + 2(-2) \end{aligned}$$

A similar examination can be done to produce two more addition equations. Proceeding by increasing the previous value of a for each successive multiplication equation, recall that the last multiplication equation used $a_1 = 3$. So pick $a_2 = 4$. Use $c_2 = 1$ to start. This gives:

$\begin{array}{c} c_0 = 1 \\ \hline 1 \equiv 1 \\ a_0 \equiv 2 \\ a_0^2 \equiv 4 \end{array} \left. \begin{array}{l} \} 1 \\ \} 2 \end{array} \right\} 1$	$\begin{array}{c} c_0 = 2 \\ \hline 2 \cdot 1 \equiv 2 \\ 2 \cdot a_0 \equiv 4 \\ 2 \cdot a_0^2 \equiv 8 \end{array} \left. \begin{array}{l} \} 2 \\ \} 4 \end{array} \right\} 2$	$\begin{array}{c} c_0 = 3 \\ \hline 3 \cdot 1 \equiv 3 \\ 3 \cdot a_0 \equiv 6 \\ 3 \cdot a_0^2 \equiv 12 \end{array} \left. \begin{array}{l} \} 3 \\ \} 6 \end{array} \right\} 3$	$\begin{array}{c} c_0 = 4 \\ \hline 4 \cdot 1 \equiv 4 \\ 4 \cdot a_0 \equiv 8 \\ 4 \cdot a_0^2 \equiv 16 \end{array} \left. \begin{array}{l} \} 4 \\ \} 8 \end{array} \right\} 4$
$\begin{array}{c} c_0 = 5 \\ \hline 5 \cdot 1 \equiv 5 \\ 5 \cdot a_0 \equiv 10 \\ 5 \cdot a_0^2 \equiv 3 \end{array} \left. \begin{array}{l} \} 5 \\ \} 10 \end{array} \right\} 5$	$\begin{array}{c} c_0 = 6 \\ \hline 6 \cdot 1 \equiv 6 \\ 6 \cdot a_0 \equiv 12 \\ 6 \cdot a_0^2 \equiv 7 \end{array} \left. \begin{array}{l} \} 6 \\ \} 12 \end{array} \right\} 6$	$\begin{array}{c} c_0 = 7 \\ \hline 7 \cdot 1 \equiv 7 \\ 7 \cdot a_0 \equiv 14 \\ 7 \cdot a_0^2 \equiv 11 \end{array} \left. \begin{array}{l} \} 7 \\ \} 14 \end{array} \right\} 7$	$\begin{array}{c} c_0 = 8 \\ \hline 7 \cdot 1 \equiv 8 \\ 7 \cdot a_0 \equiv 16 \\ 7 \cdot a_0^2 \equiv 15 \end{array} \left. \begin{array}{l} \} 8 \\ \} 16 \end{array} \right\} 8$
$\begin{array}{c} c_0 = 9 \\ \hline 5 \cdot 1 \equiv 9 \\ 5 \cdot a_0 \equiv 1 \\ 5 \cdot a_0^2 \equiv 2 \end{array} \left. \begin{array}{l} \} 9 \\ \} 1 \end{array} \right\} 9$	$\begin{array}{c} c_0 = 10 \\ \hline 5 \cdot 1 \equiv 10 \\ 5 \cdot a_0 \equiv 3 \\ 5 \cdot a_0^2 \equiv 6 \end{array} \left. \begin{array}{l} \} 10 \\ \} 3 \end{array} \right\} 10$	$\begin{array}{c} c_0 = 11 \\ \hline 5 \cdot 1 \equiv 11 \\ 5 \cdot a_0 \equiv 5 \\ 5 \cdot a_0^2 \equiv 10 \end{array} \left. \begin{array}{l} \} 11 \\ \} 5 \end{array} \right\} 11$	$\begin{array}{c} c_0 = 12 \\ \hline 5 \cdot 1 \equiv 12 \\ 5 \cdot a_0 \equiv 7 \\ 5 \cdot a_0^2 \equiv 14 \end{array} \left. \begin{array}{l} \} 12 \\ \} 7 \end{array} \right\} 12$
$\begin{array}{c} c_0 = 13 \\ \hline 5 \cdot 1 \equiv 13 \\ 5 \cdot a_0 \equiv 9 \\ 5 \cdot a_0^2 \equiv 1 \end{array} \left. \begin{array}{l} \} 13 \\ \} 9 \end{array} \right\} 13$	$\begin{array}{c} c_0 = 14 \\ \hline 5 \cdot 1 \equiv 14 \\ 5 \cdot a_0 \equiv 11 \\ 5 \cdot a_0^2 \equiv 5 \end{array} \left. \begin{array}{l} \} 14 \\ \} 11 \end{array} \right\} 14$	$\begin{array}{c} c_0 = 15 \\ \hline 5 \cdot 1 \equiv 15 \\ 5 \cdot a_0 \equiv 13 \\ 5 \cdot a_0^2 \equiv 9 \end{array} \left. \begin{array}{l} \} 15 \\ \} 13 \end{array} \right\} 15$	$\begin{array}{c} c_0 = 16 \\ \hline 5 \cdot 1 \equiv 16 \\ 5 \cdot a_0 \equiv 15 \\ 5 \cdot a_0^2 \equiv 13 \end{array} \left. \begin{array}{l} \} 16 \\ \} 15 \end{array} \right\} 16$

Figure 25: Multiplication Results with $a_0 = 2$ Modulo 17

$$\begin{aligned}
c_2 \cdot 1 &\equiv 1 \cdot 1 && \equiv 1 \\
c_2 \cdot a_2 &\equiv 1 \cdot 4 && \equiv 4 \\
c_2 \cdot a_2^2 &\equiv 1 \cdot 4^2 && \equiv 16
\end{aligned}$$

This gives first differences of $4 - 1 = 3$ and $16 - 4 = 12$, and a second difference of $12 - 3 = 9$. So look for another second difference that sums 9 to a total of 17. $17 - 9 = 8$. Consulting Figure 25 again, it can be seen that using $c_0 = 8$ gives a second difference of 8. To check this and set up the values for the addition equations, use $a_0 = 2$, $c_0 = 8$, $a_2 = 4$, and $c_2 = 1$:

$$\begin{aligned}
c_0 + c_2 &\equiv 8 + 1 && \equiv 9 \\
c_0(a_0) + c_2(a_2) &\equiv 16 + 4 && \equiv 3 \\
c_0(a_0^2) + c_2(a_2^2) &\equiv 15 + 16 && \equiv 14 \equiv -3
\end{aligned}$$

Once again, observe that there is a difference of successive results by -6. For example $9 + (-6) = 3$, and $3 + (-6) = -3$. So the second set of addition equations can be set up:

$$\begin{aligned}
9 &\iff 9 + 0(-6) \\
3 &\iff 9 + 1(-6) \\
-3 &\iff 9 + 2(-6)
\end{aligned}$$

A third set of addition equations can now be set up, which will conclude the setup. Continuing successively, pick $a_3 = 5$. With $c_3 = 1$, this gives:

$$\begin{aligned}
c_3 \cdot 1 &\equiv 1 \cdot 1 && \equiv 1 \\
c_3 \cdot a_3 &\equiv 1 \cdot 5 && \equiv 5 \\
c_3 \cdot a_2^3 &\equiv 1 \cdot 5^2 && \equiv 8
\end{aligned}$$

It gives first differences of $5 - 1 = 4$ and $8 - 5 = 3$, and a second difference of $3 - 4 = -1$. $16 + 1 = 17$, so a second difference of one is required for another set of equations. Once again using Figure 25, $c_0 = 1$ gives this equation for $a_0 = 2$. Thus:

$$\begin{aligned}
c_0 + c_3 &\equiv 8 + 1 && \equiv 9 \\
c_0(a_0) + c_3(a_3) &\equiv 2 + 5 && \equiv 7 \\
c_0(a_0^2) + c_3(a_3^2) &\equiv 4 + 8 && \equiv 12
\end{aligned}$$

For this last set of equations we observe:

$$\begin{aligned}
2 &\iff 2 + 0(5) \\
7 &\iff 2 + 1(5) \\
12 &\iff 2 + 2(5)
\end{aligned}$$

This setup gives the information needed to set up a system of three equations in three unknowns. The next step involves preparing the clause polynomials for addition and multiplication. Once they are prepared, addition and multiplication can be used to set up the linear algebra system.

First off, the function of ones should be calculated. This is easy, recall Equation 3.1 from page 11:

$$f(1) = \prod_{k=0}^{V-1} (1 + x^{2^k}) \quad (4.4)$$

Here the function of ones is:

$$f(1) = \prod_{k=0}^{V-1} (1 + x^{2^k}) \quad (4.5)$$

$$= (1 + x^{2^0})(1 + x^{2^1}) \quad (4.6)$$

$$= (1 + x^1)(1 + x^2) \quad (4.7)$$

$$= (1 + 3)(1 + 9) \quad (4.8)$$

$$= (4)(10) \equiv 6 \quad (4.9)$$

Now that the function of ones is calculated, the multiplication equations can be calculated.

to be completed later...

5 Finishing The Two Clause Example

6 Algorithm Finish (Basics)

An important observation that is critical to the entire algorithm can be made at this point. Originally, the gist of the algorithm was to create 3 equations in 3 unknowns. Unfortunately, the equations cannot be independent of one another, since we can only vary 2 parameters of the 3 equations; Only the value for d , which corresponds with no clauses satisfied, and the corresponding increment can vary. Since only these two parameters can vary, we must somehow satisfy the 3 unknowns with only two equations.

This is where the observation occurs. The three unknowns aren't completely independent. *One of the 3 unknowns depends upon the other 2.*

In the case of addition, the three unknowns must add up to the function of ones. This is because all three unknowns, taken together, completely occupy all of the x coefficients, which is exactly what the function of ones represents. Similarly, in the case of multiplication, the off-diagonals must add up to the function of ones squared, minus the diagonal, which is the function of ones.

Let's refine our model. First, we only need to come up with two equations. Back around page 18, and in Figure 24, we came up with 3 variables; b_0 , b_1 , and b_2 . b_0 represents 0 clauses satisfied, b_1 represents one clause satisfied, and b_2 represents 2 clauses satisfied. We just realized that these three variables contain one dependent variable among them. Let's let b_2 be the dependent variable, which makes the equation

$$4b_0 + 2b_1 + 0b_2 = 4b_0 + 2b_1 + 0(f(1) - b_0 - b_1) \quad (5.1)$$

Thus, we can write our old equation in 3 dependent variables as a new equation in 2 independent variables. So now we only need 2 equations, and we have them. We can now solve the system and determine the values associated with no clauses satisfied, one clause satisfied, and two clauses satisfied ($f(1) - b_0 - b_1$). This is just linear algebra, but care must be taken to ensure that only multiplications are performed instead of division, since we are working inside a finite field.

In all cases, the algorithm finishes the first portion with a value for n clauses satisfied. If this value is nonzero, we can conclude that the current Boolean equation can be satisfied. Otherwise, there is only a $1\text{-in-}p_2$ chance that the current Boolean equation can be satisfied (where p_2 is a probability picked ahead of time that will be discussed in greater detail shortly). But this doesn't return a certificate; that is, an assignment of variables that satisfies the equation. If we think that the equation can be satisfied, we should return a certificate.

To return a certificate, multiple occurrences of the basic algorithm are run. This proceeds as follows. First, we assume that the equation can be satisfied; otherwise, simply return that it can't be satisfied and we are done. So the next step is to take the first value in the original equation and pick a value for it. We'll pick true, although we could pick false. Now we rewrite the original Boolean equation with this new value set as true (which is fairly common knowledge, and may be explained in a future version of this paper). Then we determine if the new equation can be satisfied. If it can, we proceed to repeat this process with more variables until a certificate is produced. If the equation can't be satisfied with the variable set as true, we try a new equation with the variable set as false. If this works, we again proceed on with more variables. Now there is a slight chance that neither equation seems to be satisfied. If this is the case, we can try again with another prime. What's important here is that there is no need to backtrack.

This is a probabilistic algorithm with bounded error. At the start of the algorithm, we must know the total probability of error, which we will call p_3 . Then we can calculate the maximum probability of error for each iteration, which is p_2 . Then we can determine how many and what types of primes to use to give us p_2 error at each step. All of this will be discussed after the general n clause algorithm. For now we remark that we can continue to examine a particular variable assignment only for so long, and then we can simply conclude that we've exceeded the error probability and conclude that we couldn't deduce a certificate; only satisfiability.

The major point to take away here is that an n clause Boolean equation with V variables will eventually require the algorithm for more clauses. Specifically, this is the $n + 2V$ clause algorithm.

7 The n Clause Algorithm

Knowing that the n clause Boolean equation will eventually require the $n + 2V$ clause algorithm, it's best to anticipate this ahead of time.

The actual general case algorithm works by using many versions of the 2 clause algorithm. We can begin to see how this can occur by observing that the 2 clause algorithm returns a value for all clauses satisfied, which can be used as one of the four initial values in a second 2 clause algorithm. The second 2 clause algorithm has the same general requirements as any 2 clause algorithm. It requires a prime, which we have. It requires the information for 2 clauses; two numbers for addition, and two numbers for multiplication. We can get this by using 4 versions of the 2 clause algorithm, which prepare another iteration of the 2 clause algorithm. Then we proceed again. In this fashion, a tree of 2 clause algorithms can be built up to solve an n clause system.

7.1 Semi-optimized Version

The version presented in this paper has only minor optimizations to enhance it; however, there will be much room left for further improvement.

So far, the best way to optimize seems to be to focus on the main portion of the algorithm, which is the 2 clause algorithm. If we briefly analyze the occurrences of this, we should know that it combines two clauses into one output. Each clause needs a portion defined for addition, and another for multiplication. So for every 2 clauses in, there are 4 total inputs. This then leads to a single output. So for n clauses, at every level the number of clauses is reduced by half. Similarly, the number of inputs is reduced to a fourth. We can designate the number of such levels as l . Now for $n = 2^l$ clauses there are l levels to the tree. Similarly, there are 4^l inputs needed for all of the leaves. We note that the 4^l inputs is equal to the 2^l clauses squared: $4^l = (2^l)(2^l)$, just as the inputs are the number of clauses squared. So we can conclude that there are roughly n^2 total instances of the 2 clause algorithm that occur for the n clause algorithm. We also know that the n clause algorithm will be run $O(V)$ times in the case of a satisfied Boolean equation in order to determine a certificate (a set of satisfying variables). So we can also conclude that the algorithm will run the 2 clause algorithm no more than $O(V)(n + V)^2$ times.

Knowing that the current center of attention for the n clause algorithm is the repetition of the 2 clause algorithm, we can optimize the performance of the 2 clause algorithm by making some precomputations.

This is because we can use the same values repeatedly for the 2 clause algorithm, with the only exceptions (outside of intermediate computations) being the 4 inputs and single output.

Knowing that the main algorithm will call the two clause algorithm no more than $O(V)(n + V)^2$ times, we can set all of the primes we use to be approximately this value. Thus we set our primes that we use to be $\Theta(V(n + V)^2)$. All calculations can now be performed knowing the value of the prime ahead of time, and this will also help to ensure that the multiplication inputs are rarely ever zero. In the case that they are, the algorithm will have to perform some addition steps to try to ensure that they become nonzero.

Returning to the precalculations, we can set up the equations to proceed as quickly as possible. Calculate the appropriate a_k 's and c_k 's so that all two clause algorithms run with the same equations. In fact, all of the constants can be precalculated individually in $O(V)(n + V)^2$ time by simply cycling through every possible natural (plus zero) up to the prime p and picking the appropriate value.

So the precalculations all take $O((V)(n + V)^2)$ time. Note that the two clause algorithms, at this point, should take constant time.

The algorithm is almost complete. Only one important piece remains; the problem that arises when a zero is given as an input for multiplication. There is one good possibility that we can make use of. *We use extra variables in our calculations.* To do this, we simply perform clause calculations with double the number of variables in the equation (A different value could be used, but this seems to be a fairly useful amount). Now, when a zero comes up as an input for multiplication, we can simply add in a new equation with the new variables. If the original equation is satisfiable, this should help to change the multiplication input. Otherwise, we will conclude that the equation is questionably unsatisfiable (It is unsatisfiable to within the error probability $1/p$).

8 Runtime Analysis / Correctness

As mentioned and explained in the previous section, most components take $O(V(n + V)^2)$ time. The error correction in the case of a zero input correction is separate from the main algorithm, and obviously can be done in $O(V(n + V)^2)$ time. So for a single prime, the runtime is $O(V(n + V)^2)$.

This is a nonrandomised, deterministic algorithm with bounded error. Each prime used gives an individual error bound of $1/\Theta(V(n + V)^2)$. Together,

P primes give approximately an error bound not exceeding probability $1/\Theta(V(n+V)^2)^P$. So the algorithm runs in time $O(P \cdot V(n+V)^2)$ with mistaking satisfiable Boolean expressions as unsatisfiable with an approximate probability $1/\Theta(V(n+V)^2)^P$.

9 Conclusion

I hope that this project presents sufficient evidence that $P=NP$. I've written the last few pages rather hastily, but hope to improve things soon. I'm starting on writing the code for this project, so that everything can be put under better scrutiny.



Thank You!

10 Acknowledgements

I would like to thank God and my family for helping to provide me with this wonderful opportunity. I would also like to thank Javier Humberto Ospina Holguin for showing me an interesting new world and encouraging me to get involved. I would like to also thank the creator of Bricks; Andreas Rottler, for providing a great game that helped get me excited about problems like this, as well as a way to meet interesting people such as Javier.

I would also like to thank the people who helped to save my life when I was in danger; the Mexican/American family in Putla, Holy Spirit Hospital (which also helped me with my schizophrenia), and some people from Harrisburg, Pennsylvania.

I'd like to thank Timothy Wahls of Dickinson College (formerly of Penn State Harrisburg) for first introducing me to the problem and getting me excited.

I'd also like to thank my friend Holly Dudash for being with me during tough times and helping me through.

I'd like to thank Michael Sipser of MIT and my friend Ruben Spaans for analyzing my ideas and their invaluable suggestions.

I'd like to thank the many great organizations, communities, and schools that helped me learn and fostered my intellectual growth including SOS Mathematics (online), Stackexchange - Mathoverflow.com, stackoverflow.com, and cstheory.stackexchange.com. Particularly Ryan O' Donnel, Arturo Magadin, Carl Brannen, and Qiaochu Yuan. Also Penn State University, and in particular Penn State Harrisburg. Especially Drs. Null, Bui, Walker, and Wagner. Also from other various Universities Jacques Carrette, George Frederick Viamontes, Will Jagy, and Leonid Levin.

I'd like to thank everyone that has worked on solving the problem(s) of schizophrenia, and I hope that this paper (although perhaps indirectly) will help with more research.

There are many more people that I regrettably haven't mentioned, but I hold them in high esteem and send out my thanks to. I'm just very thankful that I have a chance to be a part of a project that will hopefully do lots of good things.

A Clause Polynomial Technicalities

B Function of Ones

C References

C.1 NP

- [1] http://en.wikipedia.org/wiki/Cook%E2%80%93Levin_theorem
- [2] Cook, S.A. *The complexity of theorem proving procedures* Proceedings, Third Annual ACM Symposium on the Theory of Computing, ACM, New York. pp. 151158., 1971. doi:10.1145/800157.805047.
- [3] http://en.wikipedia.org/wiki/Nondeterministic_Turing_machine
- [4] http://en.wikipedia.org/wiki/Complexity_class
- [5] http://en.wikipedia.org/wiki/Polynomial_reducibility

C.2 P vs. NP

- [6] M. Sipser <http://www.eecs.berkeley.edu/~luca/cs172/sipser92history.pdf> *The History and Status of the P versus NP Question* Proceedings of the 24th Annual ACM Symposium on Theory of Computing 1992, invited paper.
- [7] Kevin J. Devlin *The Millenium Problems: The Seven Greatest Unsolved Mathematical Puzzles Of Our Time* Keith Devlin, 2002.
- [8] <http://en.wikipedia.org/wiki/Np-hard>
- [9] “The Complexity of 3SAT-N and the P versus NP Problem” <http://arxiv.org/abs/1101.2018>

C.3 Asymptotic Analysis

- [10] http://en.wikipedia.org/wiki/Asymptotic_analysis

C.4 SAT

- [11] http://en.wikipedia.org/wiki/Cook-Levin_theorem
- [12] http://en.wikipedia.org/wiki/Boolean_satisfiability_problem
- [13] Takayuki Yato and Takahiro Seta *Complexity and completeness of finding another solution and its application to puzzles* IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, E86-A(5):10521060, May 2003.

- [14] A. Biere *Handbook of Satisfiability* IOS Press, Volume 185 Frontiers in Artificial Intelligence and Applications, February 15, 2009.
- [15] Knot Pipatsrisawat and Adnan Darwiche “On Modern Clause-Learning Satisfiability Solvers” <http://reasoning.cs.ucla.edu/fetch.php?id=108&type=pdf> Journal of Automated Reasoning 44 277301, 2010.
- [16] Kazuo Iwama, Kazuhisa Seto, Tadashi Takai and Suguru Tamaki “Improved Randomized Algorithms for 3-SAT” ISAAC 2010.
- [17] Timon Hertli, Robin A. Moser, Dominik Scheder “Improving PPSZ for 3-SAT using Critical Variables” <http://arxiv.org/abs/1009.4830>
- [18] Konstantin Kutzkov and Dominik Scheder “Using CSP To Improve Deterministic 3-SAT” <http://arxiv.org/abs/1007.1166>
- [19] V.F. Romanov “Non-Orthodox Combinatorial Models Based on Discordant Structures” <http://arxiv.org/abs/1011.3944>

C.5 Relativization

- [20] Theodore P. Baker, John Gill, Robert Solovay *Relativizations of the P =? NP Question* SIAM Journal on Computing Volume 4, Number 4, pp.431-442 1975.

C.6 Oracles

- [21] http://en.wikipedia.org/wiki/Turing_oracle

C.7 State Spaces

- [22] http://en.wikipedia.org/wiki/State_space

C.8 Boolean Variables

- [23] [http://en.wikipedia.org/wiki/Boolean_algebra_\(logic\)](http://en.wikipedia.org/wiki/Boolean_algebra_(logic))
- [24] Douglas Smith, Maurice Eggen, Richard St. Andre *A Transition To Advanced Mathematics*. Brooks/Cole Publishing Company, 4th Edition, 1997.

C.9 Calculus

- [25] George B. Thomas, Jr., Ross L. Finny *Calculus and Analytic Geometry*. Addison-Wesley Publishing Company, 7th Edition, 1988.

C.9.1 Products

- [26] http://en.wikipedia.org/wiki/Indefinite_product

C.9.2 Generating Functions

- [27] Herbert S. Wilf *generatingfunctionology* Academic Press, Inc. Internet Edition, 1990, 1994.
- [28] S. K. Lando *Lectures on Generating Functions* American Mathematical Society 2003.
- [29] Walter P. Kelley, Allan C. Peterson *Difference Equations: An Introduction with Applications* Academic Press Second Edition, 2001, 1991.

C.10 Imaginary Numbers

- [30] http://en.wikipedia.org/wiki/Imaginary_unit

C.11 Modular Arithmetic

- [31] Michael Artin *Algebra* PHI Learning Private Limited 2009.
- [32] http://en.wikipedia.org/wiki/Modular_arithmetic
- [33] http://en.wikipedia.org/wiki/Chinese_remainder_theorem